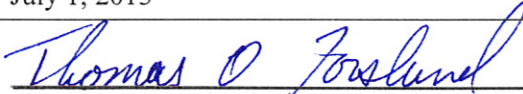


Thomas O. Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Workstation Use and Security
<b>Policy Number:</b>	S-012
<b>Effective Date:</b>	July 1, 2013
<b>Approval:</b>	<div><div> Thomas O. Forslund, Director</div><div><u>4/19/13</u> Date</div></div>

**Purpose:**

This policy establishes Wyoming Department of Health's (WDH) responsibility to ensure that workstations that access electronic protected health information are used and secured appropriately.

**Scope:**

This policy applies to all WDH workforce.

**Definition(s):**

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

**Policy:****1. General**

- a. WDH workstation users shall use and secure workstations appropriately to minimize the potential for unauthorized access and/or loss, theft, or damage.
- b. WDH workforce shall be trained on workstation use and security prior to being authorized to use workstations.
- c. If a user fails to use or secure a workstation in an acceptable manner, WDH may revoke such user's privileges, including, but not limited to, user accounts and access to secure systems, as necessary to preserve the confidentiality, integrity, and availability of electronic protected health information (ePHI).

**2. Protection from unauthorized access**

- a. Users shall apply the "lock workstation" feature (i.e., ctrl/alt/del, "lock workstation," enter) when leaving their workstations unattended.
- b. As a safeguard, workstations shall have screensavers that automatically activate after five (5) minutes of workstation inactivity.
- c. Desktop computer users shall store ePHI on a network or other approved drive (e.g., drives utilized for special program needs and approved by both a program supervisor and the WDH Compliance Office).

- d. Laptop computers must be encrypted before they are used to store ePHI. Users shall contact Enterprise Technology Services to confirm or request appropriate encryption.
- e. Users shall log off of their workstations at the end of each work day.

### **3. Physical security**

- a. Users shall protect workstations from loss, theft, or damage.
  - i. Workstations shall not be exposed to extreme heat or cold or other potentially harmful environmental conditions (e.g., rain).
  - ii. Generally, workstations should not be left unattended in a vehicle. However, if a workstation is left unattended in a vehicle, such vehicle shall remain locked, and the workstation shall not be visible and should be stored in a locked trunk (unless extreme heat prohibits such storage).

### **4. Technical security**

- a. Workstations shall be configured to reduce risk of unauthorized access to systems and the ePHI stored therein.
  - i. Workstations shall be configured according to industry standards.
  - ii. User name and password shall be required to access the operating systems within workstations.
  - iii. Mainframe terminal sessions shall be configured to log a user off the system within fifteen (15) consecutive minutes of non-use.
  - iv. Standard virus detection software shall be installed on all workstations and shall be configured to check files for viruses both before they are initially opened and routinely thereafter.
  - v. Workstation users shall neither disable nor alter technical security safeguards (e.g., virus detection software).
  - vi. Workstations shall be configured to log all significant security events (e.g., password guessing, unauthorized access attempts, modification of systems or applications).
  - vii. All information stored in workstations shall be backed up daily.

### **5. Unauthorized and malicious software**

- a. Users shall not download software applications and/or executable files to WDH workstations without prior authorization.
- b. Users shall not write, compile, copy, knowingly spread, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of any system (e.g., virus, worm, Trojan horse).
- c. Suspected viruses shall be reported immediately in accordance with WDH Policy S-005b; Protection from Malicious Software.
- d. Viruses shall not be deleted without expert assistance.

### **6. Monitoring and incident reporting**

- a. WDH reserves the right to monitor any individual user workstation either at random or for cause.
- b. Any known or suspected incident involving unauthorized access to or loss or theft of a workstation shall be reported to the WDH Compliance Office or designee.

**Contacts:**

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

**Policies:**

AS-008 and S-001b; Enforcement, Sanctions, and Penalties for Privacy and Security Violations  
AS-009 and S-006a; Report and Response to Privacy Violations and Security Incidents  
AS-010; E-mail, Facsimile, and Printer/Copier/Scanner Machines  
S-005b; Protection from Malicious Software

**References:**

45 CFR § 164.304  
45 CFR §§ 164.310(b) and (c)

**Training:**